AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1. (previously presented) An application tunneling method for establishing communication between distributed application modules in different private networks without requiring modification and administration of communication protocols of existing security protection network devices, including one or more firewall, network address translation protocol, or proxy servers, comprising:

employing a distributed communication architecture, the architecture including:

(a) at least one tunnel registration and look up service module supporting dynamic registration and access of communication data including one or more of the following types of information: (i) logical name; (ii) unique identifier; (iii) communication address; (iv) port; or (v) a service capability link pointing to a data type descriptor describing one or more of the following types of data: direct or indirect tunneling; security information; tunnel protocol type; or address mapping information for distributed application modules;

(b) at least one tunnel service software module that is independent from the existing security protection network devices to relay communication data for a local application module to an external network;

(c) at least one tunnel session that is independent from the security network protection devices and can be dynamically configured to receive messages from and send messages to different ones of the application modules and a tunnel module co-located with a session control module; and

(d) at least one tunnel message switching service supporting indirect tunneling specified in capability descriptors of tunnel sessions established between two or more remote tunnel services behind private networks;

wherein employing the distributed communication architecture results in multiple application tunnel networks over multiple private networks that have the following properties:

(a) without requiring design or configuration changes of the existing security protection network devices, the tunnel networks only require that one or more of the private networks allow for outgoing web access to one or more commonly accessible and secure web servers using a most common HTTP protocol;

(b) the tunnel networks allow dynamic selection of additional tunneling methods based on allowable inbound and outbound filtering policies of the private networks; and

(c) the tunnel networks only feed application communication module IP address, port number, and application data to tunnel service servers, thereby rendering a tunneling operation of an application independent and protected from administration of existing private networks.

2. (previously presented) The method of claim 1 wherein:

the communication data further comprises at least one of firewall restrictions, a tunnel protocol, or port mapping information obtained by a discovery module which observes the firewall restriction, interacts with an external UDP brokerage service (UBS) to allocate a port in a Network Address Translator (NAT) by sending a message to the UBS through the NAT, discovers the port mapping from the NAT through UPnP protocol and register the mapping to Look-up service;

a registration service in a public network accepts registration requests from at least one tunneling service in a private/secured network, which is connected to the public network via a firewall or network address translating device, the registration service authenticating the registering tunneling service, using certificates for processing the registration requests, and issuing registration responses to the requests;

a lookup service accepts lookup requests from at least one tunneling service in the private/secured network, and sends lookup results in response to the requests.

3. (previously presented) The method of claim 1 further comprising authenticating the communication request at a lookup service independently from private and secure network devices for at least two tunnel services to establish a secure tunnel session so that multiple communication peers can use one or more secure tunnel sessions to exchange messages through an external tunnel switching service or directly send messages to one or more ports specified in a look-up service to achieve secure tunneling of application data with dynamic selection of a tunnel switching service for indirect communication, or without tunnel switching services for direct communication to the tunnel service independent from the existing network devices.

4. (previously presented) The method of claim 3 wherein the communication request includes a certificate indicative of a network peer to allow a tunnel switching server to authenticate a message sent from a sender independently from any existing private security network devices.

5. (previously presented) The method of claim 4 wherein authenticating the communication request includes providing a tunnel identifier to the network peer in response to a certificate, wherein the tunnel identifier is used by the tunnel switching service to associate with a message queue and communication data specified in look-up services.

6. (previously presented) The method of claim 5 wherein the architecture further includes a tunnel module requesting an external tunnel switching server to create a message queue with associated session ID and certificate for one of the network peers to allows for another of the network peers to authenticate and send messages through the tunnel module to the message queue in an external tunnel switching service server in a dynamic fashion.

7. (previously presented) The method of claim 6 further comprising adding the communication request to the message queue.

8. (previously presented) The method of claim 7 wherein the message queue is a proxy queue that is created by the tunnel switching service for one remote tunnel service to receive messages from another remote tunnel service asynchronously.

9. (original) The method of claim 7 wherein creating the message queue includes creating the message queue at a server remotely located from the first network peer.

10. (previously presented) The method of claim 7 wherein creating the message queue includes creating the message queue in a tunnel switching service based on data specified in the lookup service, the tunnel services send and receive messages to and from message queues through the tunnel switching service using HTTP, SOAP or a proprietary message protocol based on a local private network security policy and firewall restrictions, and size of the messages can be reduced to support real-time traffic or increased to support large batched traffic.

11. (previously presented) The method of claim 7 further comprising tracking the location of the message queue at the lookup service so that tunnel services can use more than one message queues to receive messages to support high performance and reliability.

12. (cancelled)

13. (cancelled)

14. (previously presented) The method of claim 2, further comprising dynamically registering and selecting a tunnel protocol in a network, including:

employing a tunneling service in a private/secured network to accept data from at least one application in its local network, and forward data accepted from local applications to a tunnel switching service in an external public network through a firewall or network address translating router that connects the external public network and the private/secured network,

wherein a tunneling service in the private/secured network accepts data from the tunnel switching service in a public network via a local firewall or network address translating router, forwards the data to at least one application in its local network, and, based on content specified in the look-up service, allows two or more of the following alternatives to be selected dynamically:

(a) using HTTP to get a message from the tunnel switching server;

(b) receiving data directly from the UDP ports that is used to sent out UDP set up packet through interaction with UBS;

(c) using TCP to send and receive data;

(d) using UDP for sending and HTTP for receiving messages from a message queue in a tunnel switch;

(e) using encryption for IP address and port;

(f) using encryption for data;

(g) using new communication protocols as supported by private networks on an individual basis; or

(h) combinations of the above as supported by private networks on an individual basis.

15. (cancelled)

16. (previously presented) A lookup service in a network comprising:

a first tunnel service module that acquires communication data of an associated network peer that is connected to a first network, wherein the first tunnel service module facilitates communication between the network peer and an internetwork;

a registration table that stores the communication data and that is accessible via the internetwork; and

a second tunnel service module that sends a communication request to the registration table, acquires the communication data from the registration table, and sends a communication attempt to the first tunnel based on the communication data,

wherein said look-up service does not limit a number of entries for each communication session between two tunnel services, thereby allowing applications to group multiple message queues to create parallel communication channels between a pair of tunnel services.

17. (previously presented) The lookup service according to claim 16 further comprising a discovery module that acquires the communication data at least one of during start up of the tunnel service or based on predetermined conditions resulting in or resulting from a change of the communication data.

18. (original) The lookup service according to claim 16 further comprising a registration module that registers the communication data with the registration table.

19. (original) The lookup service according to claim 16 wherein the communication data includes at least one of a logic name, a unique identifier, a communication address, a port, a communication protocol, and service capabilities.

20. (original) The lookup service according to claim 16 wherein the communication request includes a certificate indicative of the second tunnel module.

21. (original) The lookup service according to claim 20 wherein the registration table sends a tunnel identifier to the second tunnel in response to the certificate.

22. (original) The lookup service according to claim 21 wherein the communication attempts includes the tunnel identifier.

23. (original) The lookup service according to claim 22 wherein the first tunnel verifies the tunnel identifier with the registration table and accepts the communication attempt.

24. (previously presented) The lookup service according to claim 16 wherein the first and second tunnels include a cache to store communication data to support fast access needed for dynamic selection of direct and indirect tunneling with different protocols.

25. (original) The lookup service according to claim 24 wherein the cache stores the communication data.

26. (original) The lookup service according to claim 25 wherein the cache retrieves the communication data from the registration table.

27. (original) The lookup service according to claim 16 further comprising a message queue.

28. (cancelled)

29. (cancelled)

30. (cancelled)

31. (cancelled)

32. (cancelled)

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (cancelled)

38. (cancelled)

39. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a tunneling service in a private/secured network accepting data from at least one application in its local network.

40. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a tunneling service in the first private/secured network forwarding data accepted from local applications to the tunnel switching service in the external public network through a firewall or network address translating router that connects the external public network and the private/secured network.

41. (currently amended) ~~The method of claim 38,~~ A method for establishing communications between applications in different secured or private networks comprising:

employing an application independent (web-based) tunneling service in each of the private networks, which are connected to a public network through firewall or network address translating routers;

employing a tunnel registration and lookup service in the public network;

employing a tunnel switching service in the public network; and

tunneling different application data from a first private/secured network to at least one second private/secured network,

wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in the first private/secured network forwarding data accepted from local applications to at least one second tunneling service in the second private/secured network via a first local firewall/network address translating router, the tunnel switching service in the public network to which the first local router is connected, and a second firewall/network address translating router that connects the public network to the at least one second private/secured network.

42. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in the first private/secured network forwarding data accepted from local applications to at least one second tunneling service in the second private/secured network via its local firewall/network address translating router, the public network to which the local router is connected, and a firewall/network address translating router that connects the public network to the second private/secured network.

43. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a tunneling service in the second private/secured network accepting data from the tunnel switching service in the public network via a local firewall or network address translating router.

44. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in the first private/secured network accepting data from a second tunneling service in the at least one second private/secured network via a firewall/network address translating router of the at least one second private/secured network, the tunnel switching service in the public network, and a firewall/network address translating router of the first private/secured network.

45. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in the first private/secured network accepting data from at least one second tunneling service in the at least one second private/secured network, via a firewall/network address translating router of the at least one second private/secured network, the public network connecting the private networks, and a firewall/network address translating router of the first private/secured network.

46. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a tunneling service in the at least one second private/secured network forwarding data that is accepted from the tunneling switching service in the public network to at least one application in its local network.

47. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in the first private/secured network forwarding to at least one application in its local network data that is accepted from a second tunneling service in the at least one second private/secured network, via a firewall/network address translating router of the at least one second private/secured network, the tunnel switching service in the public network, and a firewall/network address translating router of the first private/secured network.

48. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a first tunneling service in a first private/secured network forwarding to at least one application in its local network data that is accepted from a second tunneling service in the at least one second private/secured network, via a firewall/network address translating router of the at least one second private/secured network, and the firewall/network address translating router of the first private/secured network.

49. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a technique wherein at least one tunnel service in one of the private/secured networks, registers itself to a registration service in a public network, which is connected to the private/secured network by a firewall/network address translating device/router.

50. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a technique wherein at least one tunnel service in one of the private/secured networks registers at least one tunnel to a registration service in the public network, which is connected to the private/secured network by a firewall/network address translating device/router.

51. (currently amended) The method of claim [[38]]41, wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a technique wherein a first tunnel service in the first private/secured network accesses a registration service, which is connected to the first private/secured network by a firewall/network address translating device/router and the at least one second private/secured network by a firewall/network address translating device/router, to look up for a second tunnel service in the at least one second private/secured network.

52. (currently amended) ~~The method of claim 38,~~ A method for establishing communications between applications in different secured or private networks comprising:

employing an application independent (web-based) tunneling service in each of the private networks, which are connected to a public network through firewall or network address translating routers;

employing a tunnel registration and lookup service in the public network;

employing a tunnel switching service in the public network; and

tunneling different application data from a first private/secured network to at least one second private/secured network,

wherein tunneling different application data from the first private/secured network to the at least one second private/secured network includes employing a technique wherein a first tunnel service in the first private/secured network accesses a registration service, which is connected to the first private/secured network by a firewall/network address translating device/router and at least one second private/secured network by a firewall/network address translating device/router, to look up for a tunnel provided by a second tunnel service in the second private/secured network.

53. (cancelled)

54. (currently amended) The method of claim [[53]]52, wherein employing the technique to switch tunnels between different private/secured networks includes employing a lookup table in the tunnel switching service in the public network that maps at least one tunnel from at least one tunneling service in at least one private/secured network, which is connected to the public network via a firewall/network address translating device/router.

55. (currently amended) The method of claim [[53]]52, wherein employing the technique to switch tunnels between different private/secured networks includes employing the tunnel switching service that accepts data from at least one tunnel service in at least one of the private/secured networks, which is connected to the public network via a firewall/network address translating device/router.

56. (currently amended) The method of claim [[53]]52, wherein employing the technique to switch tunnels between different private/secured networks includes employing the tunnel switching service that looks up in a lookup table for a destination tunnel service for data accepted from at least one tunnel service in at least one of the private/secured networks, which is connected to the public network via a firewall/network address translating device/router.

57. (previously presented) The method of claim 56, wherein employing the technique to switch tunnels between different private/secured networks includes employing a tunnel switching service that forwards data accepted from at least one first tunnel service in at least one first private/secured network, which is connected to the public network via a firewall/network address translating device/router, to at least one second tunnel service in at least one second private/secured network, which is connected to the public network via a firewall/network address translating device/router, according to the results of lookup.